AFRL-AFOSR-UK-TR-2017-0021

Co-Modeling and Co-Synthesis of Safety-Critical Multi-threaded Embedded Software for Multi-Core Embedded Platforms

Jean-Pierre Talpin
Inst National Recherche Inform Autom

03/20/2017
Final Report

Air Force Research Laboratory
AF Office Of Scientific Research (AFOSR)/ IOE
Arlington, Virginia 22203
Air Force Materiel Command

FORM SF 298

REPORT DOCUMENTATION PAGE	*Form Approved* *OMB No. 0704-0188*

1. REPORT DATE *(DD-MM-YYYY)* 20-03-2017	**2. REPORT TYPE** Final	**3. DATES COVERED** *(From - To)* 15 May 2013 to 08 Nov 2016

4. TITLE AND SUBTITLE
Co-Modeling and Co-Synthesis of Safety-Critical Multi-threaded Embedded Software for Multi-Core Embedded Platforms

5a. CONTRACT NUMBER

5b. GRANT NUMBER
FA8655-13-1-3049

5c. PROGRAM ELEMENT NUMBER
61102F

6. AUTHOR(S)
Jean-Pierre Talpin

5d. PROJECT NUMBER

5e. TASK NUMBER

5f. WORK UNIT NUMBER

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)
Inst National Recherche Inform Autom
Domaine De Voluceau
Rocquencourt, 78150 FR

8. PERFORMING ORGANIZATION REPORT NUMBER

9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)
EOARD
Unit 4515
APO AE 09421-4515

10. SPONSOR/MONITOR'S ACRONYM(S)
AFRL/AFOSR IOE

11. SPONSOR/MONITOR'S REPORT NUMBER(S)
AFRL-AFOSR-UK-TR-2017-0021

12. DISTRIBUTION/AVAILABILITY STATEMENT
A DISTRIBUTION UNLIMITED: PB Public Release

13. SUPPLEMENTARY NOTES

14. ABSTRACT

This is the final report on the findings of the USAF/OSR grant to support collaboration between INRIA (FR), University of Kaiserslautern (DE) and Virginia Tech (VA, USA) on research entitled 'Co-Modeling of Safety-Critical Multi-threaded Embedded Software for Multi-Core Embedded Platforms. In this project, we consider and integrate two different model-based design flows that are based on synchronous languages: The first design flow starts with a polychronous model that is in some sense a process network whose nodes are triggered whenever input values are available. To ensure that such systems are deterministic and can run with bounded memory, clock consistency constraints have to be checked that are defined for the input and output streams of each node. Even if this has been successfully solved in the past individually for pure synchronous programs, and pure polychronous programs, one has to additionally determine a clock consistent schedule for the final code generation. In this proposal, we will develop new methods to ensure clock consistency in that we will reduce the problem to the constructiveness of (poly)synchronous programs. This will not only lead to new procedures to check clock consistency, but due to the constructive reasoning, we also derive schedules for code generation, and we can implement simulators for polychronous models.

15. SUBJECT TERMS
EOARD, Software modeling, Embedded systems

16. SECURITY CLASSIFICATION OF:			**17. LIMITATION OF ABSTRACT**	**18. NUMBER OF PAGES**	**19a. NAME OF RESPONSIBLE PERSON** LAWTON, JAMES
a. REPORT	**b. ABSTRACT**	**c. THIS PAGE**			
Unclassified	Unclassified	Unclassified	SAR	12	**19b. TELEPHONE NUMBER** *(Include area code)* 703-696-5999

Final report of the USAF/OSR project entitled

“Co-Modeling of Safety-Critical Multi-threaded Embedded Software for Multi-Core Embedded Platforms”

Jean-Pierre Talpin
TEA Lab
INRIA Rennes-Bretagne-Atlantique
Campus de Beaulieu
F-35042 Rennes, France

Klaus Schneider and Jens Brandt
Embedded Systems Group
Technical University of Kaiserslautern
Kaiserslautern, Germany

Sandeep Shukla
FERMAT Lab
Electrical and Computer Engineering Department
Virginia Tech
900 North Glebe Road,
Arlington, VA 22203

March 2017

NOTICE AND SIGNATURE PAGE

FOR THE DIRECTOR:

Signatures

REPORT DOCUMENTATION PAGE	*Form Approved* *OMB No. 0704-0188*

1. REPORT DATE *(DD-MM-YYYY)* 10-04-2014	**2. REPORT TYPE** FINAL REPORT	**3. DATES COVERED** *(From - To)* April 12, 2013 – April 10, 2014

4. TITLE AND SUBTITLE

Co-Modeling of Safety-Critical Multi-threaded Embedded Software for Multi-Core Embedded Platforms

5a. CONTRACT NUMBER
N/A

5b. GRANT NUMBER
FA8655-13-1-3049

5c. PROGRAM ELEMENT NUMBER

6. AUTHOR(S)
Talpin, Jean-Pierre & Schneider, Klaus & Brandt, Jens & Shukla, Sandeep K.

5d. PROJECT NUMBER

5e. TASK NUMBER

5f. WORK UNIT NUMBER

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)

INRIA INSTITUT DE RECHERCHE EN INFORMATIQUE ET
EN AUTOMATIQUE DOM VOLUCEAU BP 105
ROCQUENCOURT F-78150 FRANCE

8. PERFORMING ORGANIZATION REPORT NUMBER
N/A

9. SPONSORING / MONITORING AGENCY NAME(S) AND ADDRESS(ES)
EUROPEAN OFFICE OF AEROSPACE RESEARCH AND DEVELOPMENT
86 BLENHEIM CRESCENT, RUISLIP, MIDDLESEX HA4 7HB UNITED KINGDOM

10. SPONSOR/MONITOR'S ACRONYM(S)

11. SPONSOR/MONITOR'S REPORT

NUMBER(S)

12. DISTRIBUTION / AVAILABILITY STATEMENT
APPROVED FOR PUBLIC RELEASE; DISTRIBUTION UNLIMITED

13. SUPPLEMENTARY NOTES

14. ABSTRACT

This is the first annual report on the findings of the USAF/OSR grant to support collaboration between INRIA (FR), University of Kaiserslautern (DE) and Virginia Tech (VA, USA) on research entitled "Co-Modeling of Safety-Critical Multi-threaded Embedded Software for Multi-Core Embedded Platforms". In this project, we consider and integrate two different model-based design flows that are based on synchronous languages: The first design flow starts with a polychronous model that is in some sense a process network whose nodes are triggered whenever input values are available. To ensure that such systems are deterministic and can run with bounded memory, clock consistency constraints have to be checked that are defined for the input and output streams of each node. Even if this has been successfully solved in the past individually for pure synchronous programs, and pure polychronous programs, one has to additionally determine a clock consistent schedule for the final code generation. In this proposal, we will develop new methods to ensure clock consistency in that we will reduce the problem to the constructiveness of (poly)synchronous programs. This will not only lead to new procedures to check clock consistency, but due to the constructive reasoning, we also derive schedules for code generation, and we can implement simulators for polychronous models.

15. SUBJECT TERMS

Software Engineering, Software Producibility, Component-based software design, behavioral types, behavioral type inference, Polychronous model of computation, Prime Implicates, Boolean Abstraction, real-time embedded software, software synthesis, correct by construction software design, model-driven software design, high-assurance software

16. SECURITY CLASSIFICATION OF:			**17. LIMITATION OF ABSTRACT**	**18. NUMBER OF PAGES**	**19a. NAME OF RESPONSIBLE PERSON** WENDY HARRISON
a. REPORT U	**b. ABSTRACT** U	**c. THIS PAGE** U	U		**19b. TELEPHONE NUMBER** *(include area code)* +44(0)18956161

Contents

Foreword

Multicore processors have become standard for desktop computers since 2005, and are now also frequently used for the implementation of embedded systems. In the near future, many embedded applications including safety critical ones as used in avionics, automotive, mission control systems will run on multicore processors. For this reason, programming multicore processors should have already become a routine engineering practice. However, anybody who experienced programming of multicore processors will acknowledge the difficulty of implementing concurrent software under the currently dominating thread-based programming models: Synchronisation, deadlocks, race conditions, weak memory models, and lack of determinism of usual multithreaded software are extremely difficult to tackle. Ensuring determinism and correctness with respect to required specifications are however mandatory for safety-critical systems. For this reason, retrofitting sequential von Neumann-style programming models to multi- threaded programming is not the right way to go for programming such systems. An interesting solution to this problem is offered by model-based design methods where one can automatically generate multithreaded code from an abstract and simplified, yet formal model, using a provably 'correct-by-construction' automatic synthesis. Using the popular synchronous programming paradigms as formal models, one can reach such objectives. This way, one can formally verify the synchronous models of the systems, and once these are proved correct, code can be automatically generated for a multicore processor.

Preface

In this proposal, we consider and integrate two different model-based design flows that are based on synchronous languages: The first design flow starts with a polychronous model that is in some sense a process network whose nodes are triggered whenever input values are available. To ensure that such systems are deterministic and can run with bounded memory, clock consistency constraints have to be checked that are defined for the input and output streams of each node. One has to additionally determine a clock consistent schedule for the final code generation. In this proposal, we will develop new methods to ensure clock consistency in that we will reduce the problem to the constructiveness of (poly)synchronous programs. This will not only lead to new procedures to check clock consistency, but due to the constructive reasoning, we also derive schedules for code generation, and we can implement simulators for polychronous models.

The second design flow starts with a fully synchronous model whose reactions are triggered by a single clock. In this project, we will first develop methods to decompose such a synchronous system into components that communicate via elastic buffers instead of the otherwise used immediate broadcast communication. Then, we continue by further desynchronizing these systems in that no longer all the values are communicated between the components, but components can still locally decide when sufficiently many input values are available. Hence, a polychronous system is obtained, and we will ensure that the constructiveness of the original synchronous system is preserved during these design steps. We will additionally make sure that given temporal properties are preserved during this design flow, and we forbid decompositions that would violate these specifications.

Finally, we consider the automated multithreaded code generation for the obtained constructive polychronous models. While clock consistent schedules are already determined by our analyses, further problems have to be solved to generate efficient multithreaded code. We aim at identifying special classes of polychronous systems that simplify the code generation due to the constructive information flow of the clocks. For example, the simplest code generator is obtained for systems where the information flow of clocks follow the computation from input values to output values; (however, this is not possible for all programs). Moreover, we optimize the performance by clustering nodes into single threads, and we consider weak memory models to automatically synchronize threads where necessary taking the clock information into account.

Acknowledgement

We acknowledge the support of William McKeever, and Steve Drager from the Air Force Rome Laboratories, Wendy Harrison and James Lawton, from the USAF Office of Scientific Research, for supporting this collaborative research.

Scientific results highlights of the project

The major results of the project over the evaluated period are both scientific and economical. Scientifically, we have jointly published a series of papers [1,2,3] establishing constructive semantic foundations to co-model embedded systems using heterogeneous domain-specific languages: the polychronous data-flow language Signal and the imperative synchronous language. Reference [3], in particular, presents the first constructive semantics of polychronous systems. Based on these findings, we implemented a cross-complier, Onyx, allowing to bridge two existing synchronous programming environments: Averest (http://www.averest.org) and Polychrony, now an Eclipse-Polarsys project, https://www.polarsys.org/projects/polarsys.pop.

Economically, our project and its impact allowed us to reach new contacts with Toyota R&D, Mountain View, which yielded the start of a collaborative project described below. In 2016, Sandeep Shukla left Virginia Tech to join IIT Kanpur in India.

Visits and exchanges supported by the project

The visits and exchanges supported by the project and the co-funded INRIA associate-project POLYCORE over the funded period have been the following:

- Visit of Jean-Pierre Talpin at the Virginia Tech Research Laboratory in Arlington from April 19 to May 3, 2013.
- Visit of Jean-Pierre Talpin at the Virginia Tech Research Laboratory in Arlington from October 18 to 29, 2013.
- Visit of Jean-Pierre Talpin at the Virginia Tech Research Laboratory in Arlington from April 5 to 27, 2014.
- Visit of Jean-Pierre Talpin at the Virginia Tech, Falls Church Campus, from July 28 to September 10, 2014.
- Visit of Jean-Pierre Talpin at the Virginia Tech, Falls Church Campus, from November 4 to November 20, 2014.
- Visit of Jean-Pierre Talpin at the Virginia Tech, Falls Church Campus, from March 17 to April 2, 2015.
- Joint organizational participation to ACM-IEEE MEMOCODE’15 (Austin, Texas) from September 19 to 28, 2015.
- Joint workshop at UC San Diego, California, from November 21 to 27, 2015.

Courses and dissemination supported by the project

In the context of the above visits, Jean-Pierre Talpin was invited to give Master-class lectures at the Virginia Tech campus, Falls Church, on:

- Constructive semantics of synchronous languages, in May 2013.
- An introduction to the UML MARTE and CCSL, in October 2013.

Complementary funding obtained from the project support

In the frame of our ongoing collaboration, and thanks to the project support, we established professional contact with fellow researchers at Toyota R&D, Mountain View in late 2013. We jointly submitted a collaborative project proposal between TR&D, VTRL and INRIA. The topic of the proposal is the model-based formal verification and integration of embedded automotive architectures. The project proposal was just recently accepted and officially starts this month. We will receive funding which, in good synergy with the present project, will allow us to decouple our research and development capability and maximize the impact of our project.

Thanks to the support of the present project, we established professional contact with fellow researchers at Toyota ITC, Mountain View in late 2013. We submitted a joint project proposal to ITC, which was accepted and received an additional funding of approx. 120k$ from April 2014 to April 2015, shared between Virginia Tech and INRIA. The topic of the project is the model-based formal verification and integration of embedded automotive architectures. In the context of that project, we jointly published additional scientific articles [1,2,3], including an invited presentation at ACM DAC'15, the premier system design conference.

Joint publications supported by the project

1. "Towards refinement types for time-dependent data-flow networks". J.-P. Talpin, P. Jouvelot, S. Shukla. ACM-IEEE Conference on Methods and Models for System Design (MEMOCODE'15). IEEE, 2015.
2. "Model-Based Integration for Automotive Control Software". H. Yu, P. Joshi, J.-P. Talpin, S. Shukla, S. Shiraishi. Digital Automation Conference (DAC'15), invited presentation. ACM, 2015.
3. "Mapping Functional Behavior onto Architectural Model in a Model Driven Embedded System Design". P. Joshi, S. K. Shukla, J.-P. Talpin, H. Yu. Symposium On Applied Computing (SAC'15). ACM, 2015.
4. "Towards an architecture-centric approach dedicated to model-based virtual integration for embedded software systems (position paper)". H. Yu, J.-P. Talpin, S. Shukla, P. Joshi, S. Shiraishi. Workshop on Architecture Centric Virtual Integration (ACVI'14), 2014.
5. "Constructive Polychronous Systems". J.-P. Talpin, J. Brandt, M. Gemünde, K. Schneider, and S. Shukla. In Science of Computer Programming. Elsevier, 2014.
6. "Embedding polychrony into synchrony". J. Brandt, M. Gemünde, K. Schneider, S. Shukla, and J.-P. Talpin. In Transactions on Software Engineering. IEEE, 2013.
7. "Representation of synchronous, asynchronous, and polychronous components by clocked guarded Actions". J. Brandt, M. Gemünde, K. Schneider, S. Shukla, and J.-P. Talpin. In Design Automation for Embedded Systems, Special Issue on Languages, Models and Model Based Design for Embedded Systems. Springer, 2013.
8. "Constructive polychronous systems". J.-P. Talpin, J. Brandt, M. Gemünde, K. Schneider, and S. Shukla. Logical Foundations in Computer Science (LFCS'12). Springer, December 2012.
9. “A New Multi-Threaded Code Synthesis Methodology and Tool for Correct-by-Construction Synthesis from Polychronous Specifications”. M. Nanjundappa, M. Kracht, J. Ouy, and S. K. Shukla. In ACSD’13. IEEE, 2013.
10. “APECS: An AADL and Polychrony based embedded computing system design environment with an elevator control case study". ACM/IEEE International Conference on Formal Methods and Models for Co-Design (MEMOCODE’13). IEEE, 2013

Reset Form

FEDERAL FINANCIAL REPORT

(Follow form instructions)

1. Federal Agency and Organizational Element to Which Report is Submitted
EUROPEAN OFFICE OF AEROSPACE
RESEARCH AND DEVELOPMENT
UNIT 4515 BOX 14APO EA 09421 USA

2. Federal Grant or Other Identifying Number Assigned by Federal Agency
(To report multiple grants, use FFR Attachment)
FA8655-13-1-3049

Page 1 of 1 pages

2. Recipient Organization (Name and complete address including Zip code)
INRIA INSTITUT NATIONAL DE RERCHER EN INFORMATIQUE ET EN AUTOMATIQUE
DOMAINE DE VOLUCEAU LE CHESNAY BP105 78153 ROCQUENCOURT FRANCE

4a. DUNS Number
381909938

4b. EIN
0

5. Recipient Account Number or Identifying Number
(To report multiple grants, use FFR Attachment)
FR76 1007 1780 0000 0010 0395 848

6. Report Type
□ Quarterly
□ Semi-Annual
□ Annual
□ **Final**

7. Basis of Accounting
□ Cash □ Accrual

8. Project/Grant Period
From: (Month, Day, Year)
05/15/2013
To: (Month, Day, Year)
11/30/2016

9. Reporting Period End Date
(Month, Day, Year)
11/30/2016

10. **Transactions**	Cumulative
(Use lines a-c for single or multiple grant reporting)	
Federal Cash (To report multiple grants, also use FFR Attachment):	
a. Cash Receipts	48 039 € (60 000 $)
b. Cash Disbursements	
c. Cash on Hand (line a minus b)	
(Use lines d-o for single grant reporting)	
Federal Expenditures and Unobligated Balance:	
d. Total Federal funds authorized	48 039 €
e. Federal share of expenditures	37 254 €
f. Federal share of unliquidated obligations	0
g. Total Federal share (sum of lines e and f)	37 254 €
h. Unobligated balance of Federal funds (line d minus g)	10 785 € (11 723 $)
Recipient Share:	
i. Total recipient share required	
j. Recipient share of expenditures	
k. Remaining recipient share to be provided (line i minus j)	
Program Income:	
l. Total Federal program income earned	
m. Program income expended in accordance with the deduction alternative	
n. Program income expended in accordance with the addition alternative	
o. Unexpended program income (line l minus line m or line n)	

11. Indirect Expense	a. Type	b. Rate	c. Period From	Period To	d. Base	e. Amount Charged	f. Federal Share
					g. Totals:		

12. *Remarks: Attach any explanations deemed necessary or information required by Federal sponsoring agency in compliance with governing legislation:*

13. **Certification: By signing this report, I certify that it is true, complete, and accurate to the best of my knowledge. I am aware that any false, fictitious, or fraudulent information may subject me to criminal, civil, or administrative penalities. (U.S. Code, Title 18, Section 1001)**

a. Typed or Printed Name and Title of Authorized Certifying Official

La responsable du pôle
des chargé(e)s d'affaires financières
du centre de recherche
INRIA Rennes-Bretagne Atlantique
Carole BROSSARD

b. Signature of Authorized Certifying Official

INSTITUT NATIONAL DE RECHERCHE EN INFORMATIQUE ET EN AUTOMATISME ★
Centre de recherche
INRIA Rennes -
Bretagne Atlantique

c. Telephone (Area code, number and extension)

d. Email address

e. Date Report Submitted (Month, Day, Year)

14. Agency use only:

Standard Form 425
OMB Approval Number: 0348-0061
Expiration Date: 10/31/2011

Paperwork Burden Statement
According to the Paperwork Reduction Act, as amended, no persons are required to respond to a collection of information unless it displays a valid OMB Control Number. The valid OMB control number for this information collection is 0348-0061. Public reporting burden for this collection of information is estimated to average 1.5 hours per response, including time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding the burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to the Office of Management and Budget, Paperwork Reduction Project (0348-0060), Washington, DC 20503.

DISTRIBUTION A. Approved for public release: distribution unlimited.